Technologies sécuritaires

Poullet, Yves; Dumortier, Franck

Published in:
La protecció de dades en els estats fedrals i plurinacionals

Publication date:
2010

Document Version
le PDF de l'éditeur

TECHNOLOGIES SÉCURITAIRES: UNE RELECTURE DE LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME LA PROTECTION DES DONÉES À CARACTÈRE PERSONNEL DANS LE CONTEXTE DE LA CONSTRUCTION EN PILIERS DE L'UNION EUROPÉENE [1]

Franck DUMORTIER
Centre de Recherche Informatique et Droit des Facultés universitaires de Notre-Dame de la Paix à Namur, Belgique

Yves POULLET
Centre de Recherche Informatique et Droit des Facultés universitaires de Notre-Dame de la Paix à Namur, Belgique

INTRODUCTION

1. Dans son arrêt du 30 mai 2006 [2], la Cour de justice des Communautés européennes (CJCE) a annulé la décision de la Commission constatant la protection adéquate des données PNR [3] par les Etats-Unis et la décision du Conseil approuvant

[1] Cet article a été écrit dans le cadre de la première conférence internationale organisée par l'APCAT (Agence de protection des données de la région autonome de Catalogne (Espagne) en novembre 2006. Il figure sur le site de l'Agence: http://www.apcat.net. Il est à jour au 1er février 2007. Nous attirons l'attention du lecteur sur une récente publication disponible sur le site du contrôleur européen à la protection des données (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2007/07-02-07_preadvies_NVER_FR.pdf-score): H. HIJMANS, «Le troisième pilier dans la pratique: composer avec les faiblesses».

[2] CJCE, arrêt du 30 mai 2006, C-317/04 et C-318/04, ci-après «Arrêt PNR», disponible sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004J0317:FR:HTML.

[3] Il s'agit de l'abréviation de «Passenger Name Records», les données des dossiers passagers.

la conclusion d'un accord sur leur transfert vers ce pays, estimant que ces décisions n'étaient pas fondées sur une base juridique adéquate [4].

La question fondamentale posée à la Cour en cette occasion était celle des critères de distinction entre piliers appliqués à la protection des données à caractère personnel. Dans son arrêt, la CJCE à réaffirmé le principe selon lequel c'est bien la finalité du traitement de données qui détermine le pilier auquel celui-ci est rattaché.

Suite à cet arrêt, le Contrôleur européen de la protection des données, en abrégé, le CEPD [5] et le Groupe de l'article 29 [6] ont donné des opinions quelque peu contradictoires [7]. Peter Hustinx [8] parait conclure à la nécessité d'adopter un instrument spécifique dans le cadre du troisième pilier en déclarant que ce jugement «(...) rend d'autant plus important qu'un instrument exhaustif et cohérent sur la protection des données à caractère personnel en dehors du premier pilier soit adopté sans délai» [9]. A l'inverse, le Groupe de l'article 29 estime, quant à lui, que «l'arrêt de la Cour montre une fois de plus les difficultés dues à la division artificielle entre les piliers et la nécessité d'un cadre transpiliers cohérent en matière de protection des données» [10].

---

[4] Pour comprendre cet arrêt, il est utile de rappeler que depuis le Traité de Maastricht, l'Union européenne repose sur trois piliers: les Communautés européennes (1er pilier), la Politique étrangère et de sécurité commune (2ème pilier) et la coopération policière et judiciaire en matière pénale (3ème pilier). Ces piliers se distinguent avant tout par le mode de décision employé mais également par la compétence de contrôle de la CJCE. Ainsi, dans le 1er pilier, la procédure de décision est de type «communautaire» et implique l'ensemble des institutions. Par contre, dans les deuxième et troisième piliers, elle est de type «intergouvernemental», et le rôle du Parlement est nettement plus effacé. Sur la compétence de la Cour dans les divers piliers, voir infra n° 15.

[5] Créé en 2004, le CEPD est chargé de veiller à ce que les institutions et organes européens respectent la vie privée des personnes quand ils élaborent leurs propositions législatives. Il s'attache aussi à ce que la directive sur la protection des données de 1995 soit pleinement appliquée.

[6] Ce groupe a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE.

[7] Au sujet des relations entre le CEPD et le WP29, voy. Y. Poullet, S. Gutwirth, «The contribution of the article 29 Working Party to the construction of a harmonised European data protection system: an illustration of reflexive governance», Séminaire tenu à Bruxelles le 26 mai 2006 dans le contexte du projet intégré «Reflexive Governance in the Public Interest» supporté par le 6ème Programme-cadre de la Commission européenne et coordonné par le Prof. O. de Schutter (CDPR-UCL), à paraître.

[8] Peter Hustinx est actuellement le Contrôleur européen de la protection des données.

[9] CEPD, Communiqué de presse, *PNR-première réaction du CEPD au jugement de la Cour de justice*, 30 mai 2006, disponible sur http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2006/EDPS-2006-8-FR_PNR.pdf.

[10] WP29, Avis 5/2006 sur l'arrêt de la Cour de justice du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04 relatives au transfert de données PNR aux Etats-Unis, disponible à http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp122_fr.pdf#search=%22pnr%20vide%22.

2. Ayant rappelé la multiplication, ces dernières années, des interventions des autorités européennes dans le domaine de la lutte contre la criminalité et de la défense de la sécurité nationale (I), notre propos entend réfléchir sur la manière dont à travers, notamment mais non exclusivement, la Directive 95/46 et plus récemment la proposition de Décision-Cadre relative à la protection des données, s'établit progressivement une ligne de partage entre les traitements soumis au premier pilier et ceux soumis au troisième pilier (II). Si le mot d'ordre des autorités européennes est certes de garantir une protection des données uniforme quelque soit le pilier de rattachement des traitements en cause, nous souhaitons montrer que cette cohérence, certes ardemment souhaitée, n'est pas totale et que la division en piliers crée quelques soucis pour la cause de la protection des données (III).

I. CONTEXTE

3. Ces dernières années se sont multipliées les initiatives de l'Union européenne dans des dossiers délicats liés à la sécurité nationale et à la recherche d'infractions. La révélation par la STOA [11] des agissements du réseau Echelon [12], vaste système de surveillance satellitaire mis au point par les services secrets notamment américains et anglais ont fait craindre pour nos souverainetés nationales et ont appelé, quelques jours avant les événements dramatiques du 11 septembre 2001, à des réactions virulentes du Parlement européen [13] fondées notamment sur l'exigence d'un respect hors frontières des principes de la protection des données. La tendance dite sécuritaire qui s'est manifestée partout en Europe suite aux attentats de New York, Londres et Madrid, a largement débordé le cadre de la lutte antiterroriste [14] et a conduit à un

[11] Le STOA (Advisory Committee of the EU Parliament on Technology Assessment) publia différents rapports à propos du système de surveillance ECHELON fondés sur les révélations de journalistes tels J. BAMFORD, «The puzzle Palace» ou N. HAGER, «The Secret power», en particulier «Development of surveillance Technology and Risk of abuse of economic information», Luxembourg, Mai 1999.

[12] A propos de ce réseau d'écoutes des messages transitant par des satellites, D. YERNAULT, «L'efficacité de la Convention Européenne des Droits de l'homme pour contester le système "Echelon"», in *Sénat et Chambre des Représentants de Belgique, Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé «Echelon»*, 25 février 2002.

[13] Résolution du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système «Échelon»), 5 Septembre 2001, *JO*, n° C 072 E du 21/03/2002 pp. 0221-0229.

[14] Sur la difficulté d'une définition du terrorisme, voy. V. M. PÉREZ ASINARI, Y. POULLET, «The Airline Passenger Data Disclosure Case and the EU-US Debate», *Computer Law and Security Report*, 2002, p. 27. *«It should be clear, before any decision be adopted by EU authorities, which is the definition of "terrorism" and any other relevant concept describe in the purposes of US authorities for the processing of personal data with EU origin. This issue seems to be problematic even in the EU side: "[n] either international legal instruments, nor the Framework Decision of the Council on 13th June of 2002 concerning the fight against terrorism have really succeed in overcoming the difficulties traditionally encountered when attempting to give a definition of terrorism which describes its specificity, compared to*

renforcement des coopérations policières et judiciaires dans l'Union européenne. Ainsi, des textes nombreux ont été proposés voire adoptés en matière de lutte anti-terrorisme [15] et les transferts d'information entre les administrations chargées des contrôles aux frontières dans le cadre de VIS [16] et SCHENGEN I et II [17] ou entre les

---

other forms of organized crime in relation to all its possible forms. However, a sufficiently exact definition of the offence of terrorism is a prerequisite not only for specific indictment, but also for the application of specific procedural rules, particularly in the context of the inquiry of the investigation, and even more so for special forms of detention; otherwise the measures adopt in the fighting terrorism will lack clear legal basis, potentially bringing into question their lawfulness». EU Network of Independent Experts in Fundamental Rights, The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats, Thematic Comment drafted upon request of the European Commission, Unit A5, submitted on 31st March 2003, p. 7. See the analyses on this specific problem made in pages 11-16. See the definitions given in articles 1 and 2 by the Framework Decision of 13 June 2002 on combating terrorism, OJCE L 164, 22.6.2002, p. 4. See also the Opinion of the Economic and Social Committee on the "Commission Working Document. The relationship between safeguarding internal security and complying with international protection obligations and instruments", 2002/C 149/09, OJCE C 149, 21.6.2002, especially points 2.7, 2.9, 2.10».

[15] Ainsi, à titre d'exemple, l'initiative du Royaume de Suède en vue de l'adoption d'une décision-cadre relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, notamment en ce qui concerne les infractions graves, y compris les actes terroristes (*JO* C 281 du 18.11.2004) ou le «Traité» entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm (Allemagne), le 27 mai 2005.

[16] Proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière [COM (2005) 600 final], publiée le 24 novembre 2005. Sur cette proposition, lire l'Avis du contrôleur européen de la protection des données sur la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière [COM (2005) 600 final].

[17] Un nouveau système d'information Schengen «de deuxième génération» (SIS II) remplace SIS I et permet d'élargir l'espace Schengen aux nouveaux États membres de l'UE. Ce système comporte de nouvelles fonctionnalités. Les dispositions Schengen, élaborées sous la forme d'un cadre intergouvernemental, seront entièrement transformées en instruments juridiques européens classiques. Le 1er juin 2005, la Commission européenne a présenté trois propositions en vue de l'établissement du SIS II. Il s'agit des trois propositions suivantes:

— Une proposition de règlement fondé sur le titre IV du traité CE (visas, asile, immigration et autres politiques liées à la libre circulation des personnes) qui réglementera les aspects du SIS II relevant du premier pilier (immigration).
— Une proposition de décision fondée sur le titre VI du traité UE (coopération policière et judiciaire en matière pénale) qui réglementera l'utilisation du SIS à des fins relevant du troisième pilier.
— Une proposition de règlement fondé sur le titre V (transports) concernant spécifiquement l'accès des services chargés de l'immatriculation des véhicules aux données du SIS.

autorités de police ou les juridictions pénales dans le cadre d'institutions comme EUROPOL [18], EUROJUST [19] contribuent à la création, comme le note le CEPD, d'un «espace européen de liberté, de sécurité et de Justice». On ajoute à cela, les discussions difficiles [20] de l'article 15 de la directive «protection des données et secteur des communications électroniques» qui ont abouti à l'adoption d'une directive sur la conservation des données de communication [21] après de longues hésitations sur la nature juridique de l'instrument propre à la mise en place de cette coopération des opérateurs privés et de l'autorité publique [22].

Le Groupe de l'article 29 a ainsi noté que «l'année 2004 a été caractérisée par le conflit spectaculaire et durable entre, d'une part, les multiples tentatives des gouvernements européens et étrangers pour mettre en oeuvre de nouveaux instruments de lutte contre le terrorisme et, d'autre part, la nécessité de défendre les principes de protection des données en tant qu'élément essentiel de liberté et de démocratie. Les mesures proposées par le Conseil, les Etats membres et la Commission sont des activités qui relèvent à la fois du troisième et du premier pilier. Le Parlement européen, le Conseil et la Commission sont en désaccord sur la base juridique et, par conséquent, sur la procédure à suivre. Le Groupe de travail fait officiellement partie du premier pilier et il n'existe pas d'organisme équivalent pour conseiller le

---

Sur les accords SCHENGEN I et II, lire S. K. KARANJA, «Schengen Information System and Border Control Co-operation: A transparency and Proportionality Evaluation», Thèse, Faculté de droit d'Oslo, Juin 2006.

[18] La création d'Europol a été prévue par le traité de Maastricht sur l'Union européenne, du 7 février 1992. Installé à La Haye, aux Pays-Bas, l'Office a démarré ses activités le 3 janvier 1994. Alors connu sous le nom de «unité "Drogues Europol"» (EDU), il limitait son action à la lutte contre la drogue. Progressivement, d'autres domaines importants de la criminalité sont venus élargir ses activités. Le mandat d'Europol a été étendu le 1er janvier 2002 à toutes les formes graves de la criminalité internationale visées à l'annexe de la convention Europol.

[19] Le Conseil de l'Union européenne a adopté, le 28 février 2002, la décision instituant Eurojust, qui a succédé à Pro-Eurojust le 6 mars 2002. Cette unité, qui est dotée de la personnalité juridique, est composée d'un membre national par pays de l'Union, ayant qualité de procureur, de juge ou d'officier de police ayant des prérogatives équivalentes. Compétent pour un large champ d'infractions transnationales, Eurojust poursuit trois objectifs: «promouvoir et améliorer la coordination des enquêtes et des poursuites entre les autorités compétentes des États membres-améliorer la coopération entre ces autorités en facilitant notamment la mise en oeuvre de l'entraide judiciaire internationale; soutenir les autorités nationales pour renforcer l'efficacité de leurs enquêtes et de leurs poursuites».

[20] Sur la discussion de cet article 15 et les péripéties qui ont mené à l'adoption de la directive 2006/24/CE, lire les réflexions de E. KOSTA et P. VAELCKE, «Retaining the Data Retention Directive», *CL&SR*, 2006, pp. 370 et s.

[21] Directive 2006/24/CE du Parlement européen et du Conseil sur la rétention des données générées ou traitées dans le cadre de la fourniture de services de communication accessibles au public ou de réseaux publics de communications et modifiant la Directive 2002/58/CE (*JO* 15 Mars 2006, L 105, pp. 54 et s.

[22] A ce propos, lire Serge DE BIOLLEY, «Collecte, échange et protection des données dans la coopération en matière pénale», *JTDE*, septembre 2006, pp. 195 et s.

troisième pilier. Il existe un risque considérable que les implications de la protection des données ne soient pas pleinement prises en compte. Le Groupe de travail espère que la Commission et le Conseil réagiront rapidement à l'appel qui leur a été adressé lors de la Conférence européenne sur la protection des données avec la Résolution Wroclaw de septembre 2004 et offriront une organisation complète et efficace» [23].

4. C'est dans ce contexte d'une démarche proactive des autorités européennes, en vue de la création de cet espace européen de libertés et de sécurité, qu'une proposition de décision-cadre [24] relative à la protection des données dans le cadre du 3ème pilier a été présentée par la Commission. La proposition vise à garantir la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale entre les États membres de l'Union européenne. Son objectif est d'améliorer cette coopération, en particulier lorsqu'il s'agit de prévenir et de combattre le terrorisme, en respectant strictement les principes essentiels en matière de protection des données.

Avec raison, les autorités européennes ont-elles jugé que l'adoption d'un instrument complémentaire de protection des données, instrument lié strictement aux activités menées dans le cadre du troisième pilier, devenait nécessaire, vu les limites de la Directive 95/46 clairement rattachée au seul premier pilier.

5. On note que cette distinction entre piliers n'a jamais inquiété le Groupe de l'article 29. Ce dernier, pourtant créé dans le cadre d'une directive du premier pilier, n'a jamais limité ses compétences à celui-ci et ne s'est pas privé d'intervenir à plusieurs reprises dans des dossiers relevant du troisième pilier [25]. Cette intervention s'est faite en référence le plus souvent à l'article 8 de la Convention du Conseil de l'Europe et à

---

[23] *Ibidem*, p. 5.

[24] Proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale [SEC (2005) 1241] /* COM/2005/0475 final - CNS 2005/0202 */, disponible sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0475:FIN:FR:HTML.

[25] — **Avis 9/2004** sur le projet de décision cadre [..] (Document du Conseil 8958/04 du 28 avril 2004).

— **Avis 1/2003** sur le stockage de données relatives au trafic à des fins de facturation.

— **Avis 5/2002** sur la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff (9-11 septembre 2002), relative à la conservation systématique et obligatoire des données de trafic des télécommunications.

— **Avis 10/2001** sur la nécessité d'une approche équilibrée dans la lutte contre le terrorisme et la criminalité.

— **Avis 4/2001** concernant le projet de convention du Conseil de l'Europe sur la cybercriminalité.

— **Avis 7/2000** sur la proposition de la Commission européenne d'une directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000 COM (2000) 385.

— **Avis 10/2006** sur le traitement des données à caractère personnel par la Society for Worldwide Interbank Financial Telecommunication (SWIFT), novembre 2006.

sa jurisprudence. Ainsi dans son avis 10/2001 du 14 décembre 2001 sur une approche équilibrée dans la lutte contre le terrorisme, le groupe de travail de l'article 29 écrit à propos des mesures de lutte contre le terrorisme: «Le groupe souligne également l'obligation de respecter le principe de proportionnalité concernant toute mesure restreignant le droit fondamental au respect de la vie privée selon l'article 8 de la Convention européenne des droits de l'homme et la jurisprudence s'y rapportant. Cela implique, entre autres, l'obligation de démontrer que toute mesure prise correspond à un "besoin social impératif". Les mesures qui sont simplement "utiles" ou «souhaitées» peuvent ne pas restreindre les libertés et droits fondamentaux. Le groupe de travail souligne donc la nécessité d'organiser un débat approfondi sur les actions de lutte contre le terrorisme, en analysant toutes leurs conséquences sur les libertés et droits fondamentaux des personnes et en refusant notamment l'amalgame entre la lutte contre le terrorisme réel et la lutte contre la criminalité en général, et en limitant également les mesures procédurales empiétant sur la vie privée à celles qui sont absolument nécessaires. De plus, le groupe de travail rappelle que les mesures législatives limitant le droit des personnes au respect de la vie privée doivent être accessibles et prévisibles quant à leurs implications pour les personnes concernées. Cette exigence implique une législation suffisamment claire dans ses définitions des circonstances, de l'étendue et des modalités d'exercice des mesures d'intrusion. Les dispositions doivent être claires et détailler les circonstances dans lesquelles les pouvoirs publics sont autorisés à prendre des mesures limitant les droits fondamentaux. Elles devraient notamment spécifier où ces mesures peuvent être utilisées et devraient exclure toute surveillance générale ou préliminaire et offrir une protection contre les attaques arbitraires des pouvoirs publics».

Cette référence à l'article 8 est de même un leitmotiv des différentes interventions tant des autorités européennes que de la Cour de Justice pour justifier leur intervention et réclamer que peu importe le pilier auquel se rattache le traitement en cause, les mêmes principes, c'est-à-dire ceux déduits de l'article 8 de la CEDH s'appliquent. A cet égard, il est intéressant de relever que l'arrêt PNR commence par une référence explicite à l'article 8 lors de l'exposé du cadre juridique applicable [26], alors même que la Cour n'en fait plus aucun usage dans la suite de son jugement.

6. L'omniprésence de l'article 8 de la CEDH explique sans doute la cohérence même de l'approche suivie par les autorités européennes et la similitude de contenu des protections proposées et ce au-delà des distinctions entre piliers. Il n'empêche

---

— **Recommandation 3/99** relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit.

— **Recommandation 2/99** sur le respect de la vie privée dans le contexte de l'interception des télécommunications.

— **Recommandation 3/97** sur l'anonymat sur Internet.

[26] Voir point 3 de l'arrêt PNR, précité

que la justification des interventions européennes ne pouvait s'appuyer sur cette seule référence. Même si conformément à l'article 6 du traité de l'Union européenne, cette dernière «s'engage à respecter les droits fondamentaux des citoyens, comme garantis par la Convention européenne des droits de l'Homme et des libertés fondamentales», l'Union européenne, à la différence de ses Etats membres, n'est pas en tant que telle signataire de la Convention.

Il était donc indispensable que l'Europe se dote d'un instrument propre garantissant, au-delà des réglementations spécifiques dont on a rappelé la multiplication ces dernières années, la protection des données dans les deux autres piliers. Cette revendication exprimée dès 1998 par le Parlement européen [27] a trouvé un début de satisfaction pour le seul troisième pilier [28] par le dépôt de la décision-cadre de la Commission relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Cette proposition s'appuie sur les compétences de l'Union européenne qui relève du Titre VI du Traité sur l'Union Européenne (en abrégé TUE) et fait suite au programme de la Haye adopté par le Conseil le 4 novembre 2004 qui visait à renforcer la coopération et l'échange d'informations entre les services de police et des juridictions pénales. Dans ce contexte, le plan d'action du Conseil et de la Commission [29] invitait la Commission à présenter des propositions en matière de protection des données de manière à garantir le respect du droit fondamental à la protection des données et ce dans le cadre de cette collaboration.

II. LES CRITÈRES DE DISTINCTION ENTRE LES PILIERS APPLIQUÉS AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

1. Sur le champ d'application de la Directive 95/46

7. Alors que dans sa jurisprudence antérieure [30], la Cour semblait prendre position en faveur d'une interprétation large du champ d'application de la directive 95/46 (ci

---

[27] Ainsi, le § 25 de la résolution sur le projet de plan d'action du Conseil et de la Commission sur la meilleure manière de transposer les dispositions du Traité d'Amsterdam en matière de Libertés, Sécurité et Justice [13844/98-C4-0692/98-08/0623/CN(5), JO C 219, 30.07.1999,p. 63 et s. Cf. également sur ce point les réflexions du rapport présenté le 18 mai 2001 par G. Schmid devant le Comité temporaire du Parlement européen sur le système d'interception ECHELON], rapport sur l'existence d'un système global pour l'interception de communications (système d'interception ECHELON) (PR/439868FR.doc. PE 305.391, pp. 64 et s.).

[28] En ce qui concerne le second pilier, nos réflexions infra, n° 15 et s.

[29] Plan d'Action du Conseil et de la Commission mettant en œuvre le programme de la Haye visant à renforcer la liberté, la sécurité et la Justice dans l'Union européenne, *JO*, C 198 du 12.08.2005.

[30] CJCE, arrêt du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, point 40: «Puisque toute donnée à caractère personnel est susceptible de circuler entre les États membres, la directive 95/46 impose en principe le respect des règles de protection de telles données à

après «la Directive»), elle a considéré, dans l'arrêt PNR, que la décision d'adéquation litigieuse ne pouvait être prise sur base de la Directive étant donné que le transfert de données PNR «constitue un traitement ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal» [31].

En effet, l'article 3, § 2 de la Directive exclut de son champ d'application «le traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal» [32].

Dans son arrêt Österreichischer Rundfunk [33], la Cour avait déjà jugé qu'il ne serait pas approprié d'interpréter l'expression: «activités qui ne relèvent pas du champ d'application du droit communautaire» comme ayant une portée telle qu'il serait nécessaire de vérifier, au cas par cas, si l'activité spécifique en cause affecte directement la libre circulation entre États Membres [34]. Elle avait ensuite précisé, dans l'arrêt Lindqvist [35], que les activités exclues mentionnées dans l'article 3, § 2 le sont à titre exemplatif et que, de manière plus générale, tous les traitements mis en œuvre pour l'exercice «d'activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activité des particuliers et qui peuvent être rangées dans la même catégorie (ejusdem generis)» [36], sont exclus du champ d'application de la Directive.

8. Selon la Cour, le fait que les données PNR soient initialement collectées par les compagnies aériennes dans le cadre d'une activité qui relève du droit communautaire, à savoir la vente d'un billet d'avion qui donne droit à une prestation de services, importe peu. Selon la Cour, «au point 43 de l'arrêt Lindqvist, [il a été] jugé que les activités mentionnées à titre d'exemple à l'article 3, paragraphe 2, premier tiret, de la directive sont, dans tous les cas, des activités propres aux États ou aux autorités

---

l'égard de tout traitement de ces dernières tel que défini à son article 3», et point 42: «l'applicabilité de la directive 95/46 ne saurait dépendre de la question de savoir si les situations concrètes en cause dans les affaires au principal comportent un lien suffisant avec l'exercice des libertés fondamentales garanties par le traité et, en particulier dans lesdites affaires, avec la libre circulation des travailleurs. En effet, une interprétation contraire risquerait de rendre les limites du domaine d'application de ladite directive particulièrement incertaines et aléatoires, ce qui serait contraire à l'objectif essentiel de celle-ci, qui est de rapprocher les dispositions législatives, réglementaires et administratives des États membres afin d'éliminer les obstacles au fonctionnement du marché intérieur découlant précisément des disparités entre les législations nationales».

[31] Arrêt PNR déjà cité note 1.

[32] Article 3, § 2 de la Directive 95/46/CE

[33] CJCE, arrêt du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01.

[34] Point 42 de l'arrêt Österreichischer Rundfunk précité.

[35] CJCE, arrêt du 6 novembre 2003, Bodil Lindqvist, C-101/1.

[36] Point 43 de l'arrêt Lindqvist précité.

étatiques et étrangères aux domaines d'activité des particuliers. Toutefois, il n'en découle pas que, en raison du fait que les données PNR ont été collectées par des opérateurs privés à des fins commerciales et que ce sont ces derniers qui organisent leur transfert vers un États tiers, le transfert en cause n'entre pas dans le champ d'application de cette disposition. En effet, ce transfert s'insère dans un cadre institué par les pouvoirs publics et visant la sécurité publique» [37].

Dans cet arrêt, c'est donc bien la finalité d'exercer «des activités propres aux États au sens du point 43 de l'arrêt Lindqvist» [38], qui est prise en compte par la Cour pour déterminer si le traitement (le transfert) en question est exclu du champ d'application de la Directive. Le fait que les données aient été initialement collectées par un opérateur privé n'y change rien.

9. Cette solution semble être conforme à celle qui avait été retenue lors de l'élaboration de la directive 2006/24 relative à la rétention des données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public. Aux termes de son article 1er, la directive 2006/24 a pour objectif d'harmoniser les obligations des fournisseurs en matière de traitement et de conservation des données relatives au trafic et des données de localisation «en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne» [39].

A priori, il semble donc étonnant que le considérant 15 de cette directive stipule que «la directive 95/46/CE et la directive 2002/58/CE sont pleinement applicables aux données conservées conformément à la présente directive» [40]. En effet, la finalité répressive du traitement après la conservation des données ne fait pas de doute. Cependant, il est important de relever que l'article 4 [41], de cette directive laisse aux États membres le soin de définir eux-mêmes, dans leur droit interne, les cas et la procédure dans lesquels les données conservées peuvent être transmises aux autorités nationales compétentes.

---

[37] Point 58 de l'arrêt PNR précité.

[38] Points 52 et 58 de l'arrêt PNR précité.

[39] Article 1er de la Directive 2006/24.

[40] Considérant 15 de la Directive 2006/24.

[41] Cet article stipule que: «Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu' interprétée par la Cour européenne des droits de l'homme».

10. La directive 2006/24 ne réglemente donc que la conservation des données. Au contraire, les règles relatives à l'accès des données par les autorités compétentes relèvent du droit interne des Etats-Membres [42]. Par conséquent, conformément à la solution retenue par la Cour dans l'arrêt PNR, la directive 95/46 ne semble pas s'appliquer au transfert des données conservées (dans le cadre de la directive 2006/24) aux autorités policières et judiciaires. Tout au plus le droit interne des Etats-Membres devrait-il respecter, lors de ce transfert, les «dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu' interprétée par la Cour européenne des droits de l'homme» [43].

Il semble donc constant que le transfert de données en vue d'exercer «des activités propres aux États au sens du point 43 de l'arrêt Lindqvist» ne relèvent pas du champ d'application de la Directive. Ainsi, tous les transferts de données vers une autorité publique à des fins policières et judiciaires ainsi, qu'ils relèvent ou non de la coopération prévue par le titre VI du Traité UE, en sont exclus. De même tous les transferts de données vers une autorité étatique en vue d'activités relevant du titre V du Traité (sécurité commune) ne sont pas couverts par la Directive [44].

Pour ces raisons, l'avis [45] du Groupe de l'article 29 à propos de l'affaire SWIFT nous surprend. Rappelons que dans cette affaire largement médiatisée, le «United States Department of Treasury» (UST) a adressé des injonctions légales et contraignantes

---

[42] À cet égard, la directive 2006/24 a un champ d'application plus restreint que le projet de décision-cadre antérieur proposé par le Conseil qui comportait des dispositions supplémentaires sur «l'accès aux données retenues» et sur les demandes d'accès adressées par d'autres États membres. L'exposé des motifs explique cette limitation du champ d'application de la proposition: l'accès par les services répressifs concernés aux informations et l'échange de ces informations entre ces services sont des questions qui ne relèvent pas du champ d'application du traité CE.

[43] Article 4 de la directive 2006/24.

[44] Comme le note l'avocat général Léger dans son avis préalable à la décision PNR: «*101. It should be borne in mind that Directive 95/46, which was adopted on the basis of Article 100a of the EC Treaty, lays down protection principles which must apply to processing of personal data by any person whose activities are governed by Community law, but that, precisely because of the legal basis chosen the directive is not capable of governing State activities, such as those which concern public security or pursue law-enforcement purposes, which do not fall within the scope of Community law. (57). 102. It is true that the processing constituted by the collection and recording of air passenger data by airlines has, in general, a commercial purpose in so far as it is connected with the operation of the flight by the air carrier. Consequently, it is fair to assume that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely the sale of an aeroplane ticket which provides entitlement to a supply of services. However, the data processing which is taken into account in the decision on adequacy is quite different in nature, since it covers a stage subsequent to the initial collection of the data. It covers, as we have seen, the consultation, the use by CBP and the making available to the latter of air passenger data from air carriers' reservation systems located within the territory of the Member States*».

[45] WP29, Avis 10/2006 sur le traitement des données à caractère personnel par la Society for Worldwide Interbank Financial Telecommunication (SWIFT), novembre 2006, disponible sur http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf.

à la succursale US de SWIFT dans le contexte de la lutte antiterroriste et ensuite des évènements du 11 septembre 2001. Par ces injonctions, SWIFT se voyait intimée de fournir à l'UST un accès à certains messages transitant par son réseau et conservés au sein de son centre de traitement localisé aux USA. Bien que le transfert de certaines données bancaires détenues par SWIFT au «US Department of Treasury» dans le contexte de la lutte antiterroriste a clairement pour finalité l'exercice d'«activités propres aux États au sens du point 43 de l'arrêt Lindqvist», le Groupe n'a pas hésité à analyser la légitimité de ce transfert au regard de la Directive [46].

L'avis [47] de la Commission belge de la protection de la vie privée à propos de la même affaire nous surprend davantage encore. Dans cet avis, la Commission soutient que «le transfert de données à caractère personnel par SWIFT à l'UST ne tombe pas dans le champ d'application de l'article 3, alinéa 2 [de la Directive] parce qu'il s'agit de traitements et d'activités d'une entreprise privée, la SCRL SWIFT, et pas de traitements ou d'activités d'un Etat membre. Dans son analyse juridique susmentionnée, SWIFT atténue, à tort, sa propre contribution et minimalise clairement son propre rôle. Elle invoque une exception qui n'est prescrite que pour une action effectuée par des autorités européennes au sein du troisième pilier» [48]. Nous ne pouvons nous rallier à une telle analyse. Tout d'abord, tout comme dans l'arrêt PNR, les exigences du transfert de certaines données bancaires entre SWIFT et l'UST «se fondent sur une loi promulguée par les Etats-Unis» [49], en l'occurrence le Patriot Act. Ensuite, comme dans l'affaire PNR, cette législation «concerne le renforcement de la sécurité [...] dudit pays» [50], le traitement des données par les autorités US ayant pour finalité «la lutte contre des attentats de terroristes contre les Etats-Unis qui ont eu lieu après le 11 septembre 2001 et un réseau global de cellules terroristes qui constitueraient un risque de violence accrue contre les ressortissants, les propriétés et les intérêts américains et les intérêts nationaux et étrangers» [51]. Dès lors, il ne fait pas de doute

---

[46] *Ibidem*, p. 5: «*The independent data protection supervisory authorities within the European Union are assessing a major question relating to the transfer of financial data on a large scale from a company based in the European Union (SWIFT) to the US authorities. The details and conditions of such transfers, in particular the processing of personal data relating to individuals in Europe, have raised the concerns of DPAs who have joined forces in the investigation of the data flow and the analysis of its compliance with European privacy principles, in particular with the Data Protection Directive*».

[47] Commission de la protection de la vie privée, avis n° 47 / 2006 du 20 décembre 2006 relatif à la préparation d'une convention concernant la transmission de données à caractère personnel par SWIFT à l'US Department of the Treasury (UST), disponible sur http://www.privacycommission.be/actualites/AV47-2006.pdf.

[48] *Ibidem*, p. 8.

[49] Point 55 de l'arrêt PNR, précité.

[50] *Ibidem*.

[51] Cela ressort des informations reçues par la Commission de la protection de la vie privée. Voir l'avis 37/2006 du 27 septembre 2006 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC), p. 5.

que le transfert de données entre SWIFT et l'UST constitue «un traitement ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal» [52], au sens du point 56 de l'arrêt PNR. Le fait que les données aient été collectées, à l'origine, par une entreprise privée à des fins commerciales ne modifie en rien la finalité du transfert imposé ultérieurement par les autorités publiques à des fins de sécurité publique [53].

Ayant délimité les traitements de données relevant du premier pilier, intéressons nous à présent au champ d'application de la nouvelle proposition de Décision-Cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (troisième pilier).

2. Sur le champ d'application de la Décision-Cadre

2.1. *Application incertaine aux traitements internes*

11. L'article 1 de la nouvelle proposition de Décision-Cadre énonce que celle-ci a pour objectif de «fixer des normes communes visant à assurer la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale prévue par le titre VI du traité sur l'Union européenne».

Le sort des données transférées à des fins de coopération policière et judiciaire est donc clair, mais qu'en est-il des traitements de données ayant pour objet «la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal» [54], ne relevant pas de la coopération prévue par le titre VI du

[52] Point 56 de l'arrêt PNR, précité.

[53] Comme le note l'avocat général Léger dans son avis préalable à la décision PNR: *«101. It should be borne in mind that Directive 95/46, which was adopted on the basis of Article 100a of the EC Treaty, lays down protection principles which must apply to processing of personal data by any person whose activities are governed by Community law, but that, precisely because of the legal basis chosen the directive is not capable of governing State activities, such as those which concern public security or pursue law-enforcement purposes, which do not fall within the scope of Community law. (57) 102. It is true that the processing constituted by the collection and recording of air passenger data by airlines has, in general, a commercial purpose in so far as it is connected with the operation of the flight by the air carrier. Consequently, it is fair to assume that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely the sale of an aeroplane ticket which provides entitlement to a supply of services. However, the data processing which is taken into account in the decision on adequacy is quite different in nature, since it covers a stage subsequent to the initial collection of the data. It covers, as we have seen, the consultation, the use by CBP and the making available to the latter of air passenger data from air carriers' reservation systems located within the territory of the Member States».*

[54] On notera que la plupart des législations européennes prises en application de la Directive 95/46 couvrent aussi bien le secteur privé que public et au sein de celui-ci les traitements opérés aux fins policières, pénales et de renseignements.

TUE, qui exclues du champ d'application de la directive 95/46, ne semblent pas être couvertes non plus par la proposition de Décision-Cadre?

Consciente de ce potentiel «vide juridique» concernant les traitements policiers et judiciaires «nationaux» internes, Martine Roure [55], a souligné très justement qu'il serait opportun que la Décision-Cadre ne se limite pas aux données échangées entre Etats membres mais assure également un niveau minimal de protection des données à l'intérieur même de ceux-ci. «En effet, si cela n'était pas le cas, nous pourrions avoir deux systèmes de protection des données différents dans une même enquête. Cela menacerait non seulement la protection du citoyen mais compliquerait également le travail policier ou judiciaire» [56].

12. Dans le même esprit, dans son avis, le CEPD indiquait qu'«il est indispensable, pour la réalisation de son objectif, que la décision-cadre s'applique à toutes les données policières et judiciaires, même si elles ne sont pas transmises ou mises à disposition par les autorités compétentes d'autres États membres. Cela est extrêmement important car toute limitation concernant les données transmises aux autorités compétentes des autres États membres ou mises à leur disposition rendrait le domaine d'application de la décision-cadre particulièrement incertain et aléatoire, ce qui serait contraire à son objectif essentiel. Il serait porté atteinte à la sécurité juridique des personnes. Dans des circonstances normales, il est impossible de savoir à l'avance —c'est-à-dire au moment de la collecte ou du traitement des données à caractère personnel— si ces données seront susceptibles de donner lieu à un échange avec les autorités compétentes d'autres États membres. Le CEPD renvoie à cet égard au principe de disponibilité et à la suppression des frontières intérieures en ce qui concerne l'échange des données en matière répressive» [57].

---

[55] Martine Roure est députée au parlement européen et a été rapporteur à la Commission des libertés civiles, de la justice et des affaires intérieures pour le rapport concernant la proposition de Décision-Cadre.

[56] Martine Roure, intervention en séance plénière le 13 juin 2006. Rapport sur la protection des données dans le troisième pilier, p1. Disponible sur http://www.socialistgroup.eu/gpes/media/documents/23971_23971_roure_protection_donnees_fr_060613.PDF.

[57] CEPD, Avis du 19 décembre 2005 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (COM (2005) 475 final)(2006/C 47/12); voy. également le second avis du 26 novembre 2006 sur le même texte qui sur ce point est plus nette encore: «*For this reason,* a more limited scope is unworkable and would, if introduced, require difficult and precise distinctions within the databases of law enforcement authorities, only leading to additional complexity and costs for those authorities and moreover harming the legal certainty of individuals. *Two examples can be given to illustrate these consequences. In the first place, additional complexity and costs result from the fact that criminal files are in quite a number of cases composed of data originating from different authorities. The consequence of a limited scope would be that parts of such composed files —the parts containing data originating from authorities in other Member States— would be protected under the framework decision and that other parts would not be protected. In the second place,*

Selon le CEPD, l'article 30, § 1, *b)*[58] et l'article 31, § 1, *c)* du Traité UE constitueraient des bases juridiques adéquates pour l'adoption de règles relatives à la protection des données dont le champ d'application ne se limite pas à la protection des données à caractère personnel effectivement échangées entre les autorités compétentes des États membres, mais qui englobe aussi les situations internes[59].

13. En ce qui concerne la coopération judiciaire, l'article 31, § 1, *c)* énonce clairement que celle-ci vise, entre autres, «à assurer, dans la mesure nécessaire à l'amélioration de cette coopération, la compatibilité des règles applicables dans les États membres». Cet article semble donc permettre au Conseil d'édicter des normes visant à régir les traitements judiciaires purement internes. De plus, en matière de coopération judiciaire, comme le fait remarquer à juste titre le CEPD, la CJCE a consacré dans l'affaire Pupino[60], l'application du principe d'interprétation du droit national de manière conforme au droit communautaire.

14. Par contre, il nous semble qu'en matière de coopération policière la situation est plus incertaine. Selon l'article 30, § 1, *b)*, l'action en commun dans le domaine de la coopération policière couvrirait non seulement l'échange d'informations entre autorités compétentes mais également la collecte, le stockage, le traitement, l'analyse de ces informations par les services répressifs. Ce qui pourrait laisser penser que les traitements policiers «internes» soient visés également. Néanmoins, il importe de relever que l'article 30 ne fait que décrire ce que couvre la «coopération policière» qui, selon l'article 29, est la «coopération plus étroite entre les forces de police, les autorités douanières et les autres autorités compétentes dans les États membres (...)». A la lecture de cet article, il n'est donc pas tout

---

the legal certainty of individuals would be harmed since —in the case of a more limited scope— data originating from third countries, but not exchanged between Member States would not be covered by the Framework Decision. It goes without saying that the processing of those data entails specific risks to the data subject should there, for instance, be no legal obligation to examine the accuracy of those data. A good example would be the use of "no-fly" lists of third countries for law enforcement purposes in a Member State».

[58] Selon cet article «l'action en commun dans le domaine de la coopération policière couvre entre autres: (...) la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes, y compris d'informations détenues par des services répressifs concernant des signalements de transactions financières douteuses, notamment par l'intermédiaire d'Europol, sous réserve des dispositions appropriées relatives à la protection des données à caractère personnel».

[59] Une telle solution offrirait pour avantage que la proposition de Décision-Cadre puisse combler une part importante de la lacune déjà mentionnée de la directive 2006/24 qui ne se préoccupe pas (suffisamment) de l'accès aux données, ni de leur utilisation ultérieure après que les autorités compétentes aient pu y accéder à des fins répressives. Ainsi la Décision-Cadre prendrait le «relais» de la directive 95/46 à partir du moment où les données conservées en application de la directive 2006/24 sont transférées aux autorités compétentes, c'est à dire à partir du moment où les données sont «passées» du 1er au 3ème pilier.

[60] CJCE, arrêt du 16 juin 2005, Pupino, C-105/03.

à fait évident que l'article 30, § 1, *b)* soit destiné à régir également les traitements policiers purement internes [61].

L'incertitude quant à l'étendue du champ d'application de la proposition de Décision-Cadre a même été explicitement reconnue par le Conseil dans sa dernière version du projet [62]. On peut y lire que cinq Etats Membres [63] sont d'avis que le champ d'application de la proposition devrait être limité à l'échange de données entre Etats Membres et ne devrait pas couvrir les données traitées dans un contexte purement interne. L'Espagne est, du même avis, mais reconnaît toutefois que les règles de transfert entre Etats Membres puissent, en général, avoir un effet sur les règles applicables aux traitements internes.

En l'absence de disposition plus précise que l'actuel article 1, l'étendue du champ d'application de la proposition reste donc incertaine. On note que cette incertitude ne pourrait être levée par la Cour de Justice que de manière très disparate étant donné que, dans le cadre du 3ème pilier, sa compétence de statuer sur des questions préjudicielles dépend d'une déclaration des Etats-membres acceptant cette compétence [64].

2.2. *Non-Application de la proposition de Décision- Cadre au deuxième pilier*

15. Ainsi que le note le CEPD dans son premier avis, la proposition de Décision-Cadre ne s'applique pas aux traitements réalisés dans le cadre du deuxième pilier du traité UE (politique étrangère et de sécurité commune) ni aux traitements de données par les services de renseignement, ni à l'accès de ces services à ces données lorsque celles-ci sont traitées par les autorités compétentes ou d'autres parties (ceci découle de l'article 33 du traité UE).

Dans ces domaines, c'est donc le droit national des Etats-Membres qui doit garantir une protection appropriée des personnes concernées en respectant, en principe, les prescrits de l'article 8 de la CEDH.

Il s'agit là d'une lacune non négligeable de la proposition de Décision-Cadre dans la mesure où tous les traitements dans le domaine répressif ne peuvent pas être pris

---

[61] Nous partageons néanmoins la considération du CEPD selon laquelle «*il est tout indiqué d'aborder dans une même proposition les données des services de police et celles des autorités judiciaires traitées à des fins répressives. En premier lieu, le passage de l'enquête pénale aux poursuites n'est pas organisé de la même manière dans les États membres, les autorités judiciaires intervenant à des stades différents. En deuxième lieu, il est possible que toutes les données à caractère personnel traitées au cours de cette procédure finissent par figurer dans un dossier judiciaire. Il n'est donc pas logique d'appliquer des régimes différents régissant la protection des données lors des étapes évoquées ci-dessus*».

[62] Disponible sur http://www.statewatch.org/news/2006/nov/eu-dp-13246-rev5-06.pdf.

[63] Il s'agit de CH, CZ, DK, IE et UK.

[64] Voir *infra*, n° 31.

en considération à l'échelle de l'UE et vu le contexte de «lutte contre le terrorisme» dans lequel se sont engagées les autorités de l'Union.

16. En effet, dès le lendemain des attentats 11 septembre 2001, les autorités de l'UE soulignèrent la nécessité d'approfondir la coopération entre agences ou services de renseignements. Ainsi, le 14 septembre, la déclaration commune des chefs d'Etat et de gouvernement de l'UE promettait que «dans la lutte contre le terrorisme, nous développerons nos efforts en matière de renseignements» [65]. Peu après, le Conseil Justice et Affaires intérieures (JAI) a adopté un long catalogue d'intentions dont un chapitre est d'ailleurs spécifiquement intitulé «coopération policière/services de renseignement» [66]. Le 19 octobre 2001, le Conseil européen confirmait sa détermination à combattre le terrorisme «par exemple en renforçant la coopération entre les services opérationnels chargés de la lutte contre le terrorisme: Europol, Eurojust, les services de renseignements, les services de police et les autorités judiciaires».

Au niveau structurel, outre EUROPOL et EUROJUST, relevant du 3ème pilier, il existe un certain nombre d'«agences», formelles ou moins formelles, collaborant dans la lutte contre le terrorisme et relevant des différents piliers de l'Union. Ainsi, dans la foulée du traumatisme madrilène, les chefs d'Etat et de gouvernement des Etats membres de l'UE ont créé un poste de «coordinateur de la lutte antiterrorisme» dont la fonction principale est de coordonner la lutte au niveau européen, et d'assurer une optimisation du partage de l'information entre les différents Etats membres, mais aussi avec les pays tiers. Tant la base légale que le mandat précis du coordinateur ne sont pas très clairs [67]. Notons également la collaboration dans la lutte contre le terrorisme de la «Task force des commissaires de police» [68], relevant apparemment

---

[65] Déclaration commune des chefs d'Etat et de gouvernement de l'UE du 14 septembre 2001.

[66] Ce chapitre précise: «le Conseil rappelle l'importance, pour la qualité des analyses d'Europol, d'une transmission rapide par les autorités policières, mais aussi par les services de renseignement des Etats membres, de toute donnée pertinente en matière de terrorisme, conformément aux dispositions de la Convention Europol. (...) Le Conseil souligne le rôle important des services de sécurité et de renseignement dans la lutte contre le terrorisme. Les informations qu'ils fournissent représentent un atout inestimable pour révéler à un stade précoce d'éventuelles menaces terroristes ou intentions de terroristes ou groupes terroristes. Ces services ont par conséquent une mission essentielle dans la prévention du terrorisme. La coopération et l'échange d'informations entre eux doivent être intensifiés. Afin d'accélérer ce processus, les responsables de ces services dans les Etats membres de l'Union européenne se réuniront régulièrement dès avant le 1er novembre 2001. Ils prendront sans retard les mesures nécessaires pour améliorer ultérieurement leur coopération. La coopération entre les services de police, y compris Europol, et les services de renseignement devra être renforcée».

[67] Sur ce point, voy. House of Lords European Union Committee, 5th report of Session 2004-2005, *After Madrid: the EU's Response to Terrorism*, p. 25 et s.

[68] La «Task force des commissaires de police» a été mise en place suite au sommet de Tampere en octobre 1999. La recommendation n°44 prévoyait: «the establishment of a European Police Chiefs Operational Task Force to exchange, in cooperation with Europol, experience, best practices and

du troisième pilier, mais dont la base légale n'est pas très précise [69], et dont l'objectif est de créer une structure d'échange et de coordination au niveau des différents chefs des services de police en Europe. Citons ensuite SitCen, une agence relevant du second pilier, qui, selon le programme de la Haye [70], présentera au Conseil, à compter du 1er janvier 2005, «une analyse stratégique de la menace terroriste fondée sur les renseignements transmis par les services de renseignement et de sécurité des Etats membres et, s'il y a lieu, sur des informations fournies par Europol» [71]. Enfin, mentionnons le cas de l'«agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures» (FRONTEX), relevant, elle, du premier pilier, qui travaille en liaison étroite avec EUROPOL, le CEPOL et l'OLAF afin de renforcer la sécurité aux frontières en assurant la coordination des actions des États membres dans le cadre de la mise en œuvre des mesures communautaires relatives à la gestion des frontières extérieures.

17. Le paysage «institutionnel» de la lutte antiterroriste offre donc une combinaison de structures relevant des trois piliers. Outre le fait que les bases légales sur lesquelles ces agences sont fondées ne sont pas toujours certaines et font craindre un manque de contrôle effectif, la collaboration entre ces différentes structures pose évidemment d'importantes questions relatives aux règles applicables aux transferts de données entre celles-ci. L'on peut, par exemple, se demander quel cadre légal s'applique à l'échange d'informations entre Europol et SitCen ou encore entre EUROPOL et la «Task force des commissaires de police». De manière plus générale, on peut également se poser la question de savoir quelle institution européenne est compétente pour superviser le respect des droits fondamentaux lors de ces transferts transpiliers, dès lors que ni le Groupe de l'article 29 ni le CEPD n'ont reçu de compétences formelles dans ces domaines.

18. Le fait que la proposition de décision-cadre ne couvre pas les traitements et les transferts de données impliquant les structures relevant du second pilier est donc une lacune majeure dans le contexte de la lutte antiterroriste. Si au niveau national, les Etats-Membres sont bien sûrs dans l'obligation de respecter l'article 8 CEDH, il n'en reste pas moins que nombre de transferts, entre agences, de données «à finalité répressive» sont dépourvus de cadre légal cohérent relatif à la protection des don-

---

information on current trends in cross-border crime and contribute to the planning of operative actions».

[69] Sur ce point lire l'analyse de **Tony Bunyan** de **Statewatch**, qui examine l'émergence et le rôle de la «Task force» des commissaires de police européens et du Comité des commissaires de police, «*a tale of self-regulation and self-definition by a body with no legal or constitutional basis. Police Chiefs Committee created*», disponible sur http://www.statewatch.org/news/2006/mar/pctf.pdf.

[70] Programme de la Haye, disponible sur http://ec.europa.eu/justice_home/news/information_dossiers/the_hague_priorities/doc/hague_programme_fr.pdf.

[71] Programme de la Haye, point 2.2, p. 29.

nées à caractère personnel. Tout au plus, existe(ra)-t'il des accords particuliers [72], fixant les principes de base à respecter, ce qui n'élude cependant pas les questions d'incertitude juridique, de déficit de «contrôle démocratique» et de «recours effectifs» des citoyens, étant donné que, dans le second pilier, la compétence de la CJCE est encore plus restreinte que dans le troisième.

3. Récapitulatif des critères de distinction entre traitements rattachés au 1er pilier et traitements rattachés au 3ème pilier

19. Petit à petit, s'établit donc une ligne de démarcation entre traitements soumis respectivement aux premier et troisième piliers. Ainsi, tous les traitements effectués par une autorité étatique à des fins policières et judiciaires ainsi que les transferts de données vers ces autorités, qu'ils relèvent ou non de la coopération prévue par le titre VI du Traité sont exclus du champ d'application de la Directive 95/46, tout comme les traitements de données effectués par ces autorités dans le cadre du titre V du Traité à des fins de sécurité commune. La proposition de Décision-Cadre s'appliquera, quant à elle, de manière certaine aux transferts de données effectués dans le cadre de la coopération policière et judiciaire en matière pénale. Son applicabilité aux traitements policiers et judiciaires purement «internes» semble toutefois plus incertaine. A l'image de cette controverse, la proposition ne couvrira d'ailleurs pas l'ensemble des traitements ayant une «finalité répressive» étant donné que son champ d'application ne s'étend pas aux traitements effectués dans le cadre du second pilier.

II. UNE DISTINCTION À RELATIVISER: L'UNITÉ DES PRINCIPES DE PROTECTION DES DONNÉES

20. On ajoutera —et ce point est souligné tant par le Groupe de l'article 29 que par le CEPD— que si distinction il y a, les auteurs de la proposition de décision-cadre [73] insistent sur le fait que les deux textes obéissent aux mêmes principes, ce qui a

---

[72] Voy. par exemple la proposition de décision du Conseil [COM (2006) 817 final] portant création de l'Office européen de police (Europol) dont l'article 22 stipule qu'elle s'appliquera aux échanges d'information entre Europol et certaines autres agences européennes dont notamment FRONTEX et OLAF.

[73] «Le Parlement européen (Point 1h) d'une proposition de recommandation du parlement européen à l'intention du Conseil sur l'échange d'informations et la coopération concernant les infractions terroristes (2005/2046(INI), adoptée le 7 juin 2005) a recommandé l'harmonisation des règles existantes en matière de protection des données individuelles dans les instruments du troisième pilier, en les regroupant au sein d'un seul instrument qui garantisse un niveau identique de protection des données que celui prévu dans le cadre du premier pilier» (Exposé des motifs précédant la proposition de décision cadre déjà citée, p. 3).

pour effet de garantir aux citoyens la cohérence d'approche de l'ensemble des traitements et permet d'éviter que les traitements du 3ème pilier puisse suivre des règles qui s'écarteraient des principes reconnus dans le premier pilier et déjà largement interprétés par les autorités nationales et européennes de protection des données. «L'adoption de cette proposition constituerait un pas en avant considérable pour la protection des données à caractère personnel dans un domaine important qui requiert, notamment, un mécanisme cohérent et efficace capable de garantir la protection des données à caractère personnel à l'échelle de l'Union européenne».

21. Ainsi, les définitions proposées rejoignent point par point celles de la directive 95/46/CE. Le CEPD ne manque pas de souligner, à propos de la plupart des dispositions, leur conformité «à la législation de l'Union européenne en matière de protection des données[74]». Ainsi, les dispositions relatives à la qualité des données reprises à l'article 4 sont quasi similaires à celles de l'article 6 de la Directive 95/46/CE; même remarque, à propos des droits de la personne concernée visée par les articles 19 à 22 de la proposition, du principe de sécurité visé par les articles 23 et suivants de la proposition où on retrouve nombre d'expressions semblables à celles de l'article 16 de la Directive. On évoquera le parfait parallélisme des dispositions relatives au «Groupe de protection des personnes à l'égard des traitements des données à caractère personnel à des fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière», défini à l'article 31 de la Proposition et celles du Groupe dit de l'article 29 institué par la Directive 95/46/CE[75]. Même remarque à propos des articles de la proposition, relatives aux recours, à la responsabilité et aux sanctions directement copiés des articles 21 et suivants de la directive 95/46/CE.

22. L'intérêt d'une lecture comparative serrée des deux textes, la proposition et la Directive mère, amène d'ailleurs le CEPD à deux types de réflexions. Ayant admis une cohérence globale de contenu des deux instruments, premièrement, il pointe cependant quelques oublis ou lacunes de la proposition vis-à-vis de la Directive et,

---

[74] Ce qui inclut outre les Directives 95/46, 2002/58 et 2006/24, le règlement européen n° 45/2001 et les nombreux textes disparates élaborés dans le cadre du troisième pilier à propos de SCHENGEN, EUROPOL, EUROJUST, VIS, etc., en tout cas l'article 8 de la Convention européenne des droits de l'Homme, la Convention n° 108 et l'article 8 de la Charte européenne des droits de l'Homme.

[75] Sans doute certaines distinctions peuvent malgré tout être trouvées. Sur celles-ci et notre regret de voir mettre sur pied deux groupes différents suivant les piliers, ce qui risque d'aboutir à des incohérences d'interprétation sur des principes pourtant communs, lire nos rélexions in Y. POULLET, S. GUTWIRTH, «The contribution of the article 29 Working Party to the construction of a harmonised European data protection system: an illustration of reflexive governance», Séminaire tenu à Bruxelles le 26 mai 2006 dans le contexte du projet intégré «*Reflexive Governance in the Public Interest*» supporté par le 6ème Programme-cadre de la Commission européenne et coordonné par le Prof. O. DE SCHUTTER (CDPR-UCL), à paraître.

secondement, il note quelques ajouts ou précisions heureux. Sur le premier point, le CEPD note par exemple l'absence de dispositions relatives aux systèmes de décisions automatisés [76], la rédaction maladroite de l'article 4 qui permettrait de traiter des données qui «faciliteraient» le travail d'enquête policière ou judiciaire, sans être à strictement parler «nécessaires» à ce travail [77].

Le second point est plus important. Le CEPD insiste sur l'intérêt de compléter [78] les dispositions de la Directive 95/46/CE chaque fois que les spécificités du secteur y invitent. Il note ainsi l'importance de la fiabilité, de l'exactitude des données ainsi que de leur proportionnalité, étant donné les conséquences graves que peut avoir tout défaut de qualité de ces données. Le principe de la distinction des données fondées sur des opinions ou appréciations personnelles introduit à l'article 4.1.*d)*, l'obligation suivant l'article 4.3. de distinguer parmi les personnes concernées reprises dans les traitements policiers ou judiciaires, des catégories (suspects, témoins, condamnés, etc.), le rappel du principe de proportionnalité du traitement policier ou judiciaire qui, selon l'article 4.4., ne peut être opéré que s'il n'existe d'autre moyen moins attentatoire à la vie privée de la personne concernée, les limites sévères à la durée de conservation des données, limites introduites par l'article 7 de la proposition et l'obligation (article 9 de la proposition) de vérification des données lors de transmission permettent de manière heureuse de limiter ces risques.

Même remarque à propos de l'obligation de sécurité tant la prévention des risques d'accès non autorisés en matière de données policières et judiciaires est une priorité. La «journalisation et l'enregistrement d'une trace documentaire», en d'autres termes la tenue systématique des log-in d'accès en lecture ou en écriture dans les bases de données policières et judiciaires prévue par l'article 10 de la Proposition, apparaît comme un complément ou une suite évidente de l'obligation générale de prise de mesures de sécurité appropriées, prévue tant par la Convention n° 108 que par l'article 16 de la Directive.

L'article 19.2, l'article 20.2 et l'article 21.2 précisent les hypothèses où le droit à l'information, pour les deux premiers articles cités, le droit d'accès, pour le troisième de la personne concernée pourront être refusés, heureuse précision lorsqu'on sait la façon dont les droits nationaux ont parfois étendu les possibilités de refus d'accès de manière disproportionnée.

---

[76] Premier avis du CEPD, déjà cité, n° 126 et s.

[77] *Ibidem*, n° 72 et s.

[78] *Ibidem*, Conclusions 1, «Les règles supplémentaires (qui complètent les principes généraux établis dans la Directive 95/46/CE) devraient offrir aux personnes concernées une protection supplémentaire dans le cadre spécifique du troisième pilier, mais ces règles supplémentaires ne peuvent pas entraîner un niveau de protection inférieur».

Au nom de cette spécificité des traitements policiers et judiciaires, le CEPD n'hésite pas à suggérer l'ajout de certaines dispositions. En ce qui concerne les données sensibles, l'article 6 reprend la liste des données de l'article 8 de la directive 95/46/CE. Pourquoi ne pas y ajouter les données biométriques et les profils ADN [79] potentiellement sensibles et dont l'utilisation est fréquente dans le secteur visé. Autre exemple: le CEPD [80] plaide pour un élargissement des possibilités d'usage ultérieur des données, étranger aux finalités initiales de la collecte: «La proposition ne tient pas compte de manière tout à fait satisfaisante d'une situation à laquelle les services de police peuvent être confrontés dans le cadre de leurs activités, à savoir la nécessité d'utiliser ultérieurement des données pour une finalité considérée comme incompatible avec celle pour laquelle elles ont été collectées».

III. UNE DISTINCTION CEPENDANT NON EXEMPTE DE RISQUES

1. Une division peu évidente au regard des renforcements des coopérations entre les pouvoirs privés et publics

23. Sans doute peut-on considérer que la division opérée par la Cour de Justice des communautés européennes entre traitements soumis respectivement aux troisième et premier piliers trouve leur fondement dans une lecture attentive des prescrits européens. Il n'empêche que la distinction semble un peu artificielle dans la mesure où la finalité de sécurité publique ou de lutte contre les infractions se réalisent de plus en plus à travers une collaboration des pouvoirs publics et privés. A cet égard, l'exemple de la Directive 2006/24 est intéressant. Ainsi que nous l'avons déjà relevé, le rattachement de cette directive au premier pilier se justifie par les limites de son champ d'application qui est restreint aux seuls traitements de conservation par les fournisseurs de services de communication visés par la Directive, à l'exclusion de l'accès par les autorités de police et judiciaires à ces données ainsi conservées.

On notera que cette distinction entre les traitements de conservation et de mise à disposition résiste mal à la critique adressée par la CJCE à la décision PNR. Si le critère de répartition entre le premier pilier et le troisième est la finalité, il eût été normal de dire que les traitements de conservation tombent sous le troisième pilier dans la mesure où leur finalité est exclusivement de faciliter la poursuite d'infractions à l'exclusion de toute autre finalité (suivi de la clientèle, marketing...) à laquelle cette masse d'informations pourrait servir.

Certes, on peut arguer de l'existence d'une distinction théorique entre les moments de cette coopération. Le premier moment, celui de la conservation des données, vise

[79] *Ibidem*, n° 80.

[80] *Ibidem*, Conclusions point o).

les entreprises opératrices de services de communication et a pour finalité, dira t'on, la mise à disposition éventuelle de données; le second moment consiste en la mise à disposition effective et ce qui suit cette mise à disposition et vise cette fois les autorités policières ou judiciaires habilitées.

24. Deux finalités donc et deux régimes différents: le premier, la directive 95/46 et le second, la Décision-Cadre. Mais cette distinction se heurte à la réalité et d'aucuns soulignent le caractère artificiel de la division. Il est clair que la rétention, ses modalités et son étendue sont entièrement déterminées par la façon dont on souhaite régler l'accès [81]. Bref, la directive «Data Retention» n'a de sens que si la future Décision-Cadre s'applique également aux traitements «internes» et prévoit des dispositions fixant les questions de l'accès aux données (Qui? Moyennant quelles autorisations? A quoi? Pour quelles finalités?) et aborde la question du formatage des données à transmettre.

Le cas PNR est loin d'être isolé. On connaît la tendance de certains gouvernements de libéraliser certaines fonctions de police (surveillance des prisons, signalement des infractions, etc.). Faudra t'il dans ces cas là régler distinctement les traitements suivant la qualité de la personne qui détient les données dans un premier temps et dans un second temps, alors même que la finalité des traitements est la même et se poursuit à travers ces différents traitements? A cet égard, on apprécie la solution proposée par le rapport Rouvre adressé au Parlement européen et sa suggestion d'un ajout au projet de décision-cadre et ce à propos des traitements opérés par des entreprises privées en relation avec des administrations publiques: «Member States shall lay down in their national legislation that, where private parties collect and process data in connection with public administration, they are subject to obligations which are either equivalent to or stricter than those imposed on the competent authorities».

25. Par ailleurs, comment régler les cas de plus en plus nombreux où les autorités policières, judiciaires voire les services de renseignements exigent, en fonction de dispositions réglementaires comme celles relatives à la lutte contre le blanchiment d'argent, l'accès à des données détenues par des autorités privées. Comme le note le CEPD dans son avis sur le projet de décision cadre, l'échange de données à caractère personnel avec des personnes privées est à double sens. Il implique aussi que des données à caractère personnel sont transmises à des services répressifs et des autorités judiciaires ou mises à la disposition de ceux-ci par les personnes privées. Dans ce cas, des autorités publiques accèdent à des données à caractère personnel qui ont été collectées à des fins commerciales (transactions commerciales, marke-

[81] Certains auteurs s'interrogent même sur l'identité du responsable du traitement dans la mesure où la finalité et les moyens (données à conserver, durée de conservation...) sont entièrement déterminés par la loi en fonction des besoins légitimes de l'autorité policière).

ting, fourniture de services etc.) et sont gérées par des responsables du traitement privés, et utilisent ultérieurement ces données pour les finalités très différentes, que constituent la prévention et la détection des infractions pénales, et les enquêtes et les poursuites en la matière. On note que cette mise à disposition peut être au bénéfice direct d'autorités publiques étrangères qui peuvent en fonction de leurs propres législations intercepter des communications ou exiger la production d'informations à des fins de sécurité nationale ou de lutte contre des infractions. A cet égard, outre le cas PNR, on citera le cas SWIFT récemment à la une de l'actualité [82].

26. La réglementation applicable à de tels cas de transmission à des autorités publiques européennes ou internationales n'est pas évidente [83].

En ce qui concerne les transfert de données d'opérateurs privés vers des autorités publiques européennes, on note l'existence de l'article 13 de la directive 95/46 qui autorise les Etats membres «à prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 § 1, à l'article 10, à l'article 11 § 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder: *a)* la sûreté de l'Etat; *b)* la défense; *c)* la sécurité publique, *d)* la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas de professions réglementées...».

Qu'est-ce à dire si ce n'est que dans le cadre de cette «coopération» public-privés, la directive 95/46 s'est déclarée compétente en permettant aux Etats Membres de prendre des mesures pour faire bénéficier l'entreprise privée de toute une série de dérogations en particulier en ce qui concerne le droit à la transparence vis-à-vis des personnes concernées et même en ce qui concerne les exigences relatives à la légitimation des traitements. Sans doute, ces exceptions dans le chef des entreprises communicantes devraient s'accompagner de limites imposées cette fois dans le chef du destinataire de ces informations qui devraient ne pouvoir les exiger et n'y avoir accès que dans le respect de principes analogues qui lui seraient imposés par la décision-cadre en gestation. C'est cette lacune dans l'actuelle proposition de directive que le CEPD met en évidence en affirmant: «Tant que cet aspect n'est pas traité dans le premier pilier, un instrument relevant du troisième pilier pourrait prévoir la protection nécessaire. Cette position du CEPD se trouve encore renforcée par l'augmentation générale des échanges de données entre États membres et par la récente proposition relative au principe de disponibilité. Des dispositions nationales différentes en matière d'accès et d'utilisation ultérieure ne seraient pas compatibles avec la «libre circulation», à l'échelle de l'UE, des informations en matière répressive qui est proposée et qui vise également les données provenant de bases de données privées. Dès

[82] A ce propos l'avis de la CPVP du 27 septembre 2006 publié sur le site de la Commission belge.

[83] Voir aussi *supra* point 10.

lors, le CEPD estime que des normes communes devraient s'appliquer à l'accès des services répressifs aux données à caractère personnel détenues par des personnes privées, de façon à garantir que l'accès ne soit autorisé que sur la base de conditions et de restrictions clairement définies. En particulier, les autorités compétentes ne devraient pouvoir accéder aux données qu'au cas par cas, dans des circonstances précises et pour des finalités données et cet accès devrait faire l'objet d'un contrôle juridictionnel dans les États membres» [84].

27. Le cas d'une injonction en provenance directe d'un Etat tiers soulève d'autres questions encore. On relève que dans le cadre de la négociation du Safe Harbor, curieusement, la question de l'impact de l'existence de réglementations obligeant les entreprises bénéficiant du Safe Harbor sur le caractère adéquat de la protection offerte par les Safe Harbor semble avoir été résolue de manière négative. L'alinéa 4 de l'annexe 1 de la décision de la Commission 2000/520/CE [85], qui fixe les Principes de la sphère de sécurité affirme que «l'adhésion aux principes peut être limitée par les exigences de la sécurité nationale, l'intérêt public et le respect des lois des Etats-Unis...». En d'autres termes, la décision d'adéquation sur base du premier pilier n'est pas remise en cause par une décision ultérieure de l'Etat considéré adéquat dans la mesure où celle-ci s'appuie sur des raisons de sécurité nationale et peut trouver son fondement dans une loi du pays du destinataire. Cette position semble récemment avoir été remise en cause par le Groupe de l'article 29 lors de son avis concernant la législation américaine SARBANNES-OXLEY du 1er février 2006 [86]. Il s'agissait en l'occurrence de savoir dans quelle mesure une entreprise soumise à la Directive ou plutôt les employés de cette entreprise étaient ou non tenus par l'obligation légale américaine de signaler les malversations et certaines infractions commises dans les domaines bancaire, de comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et les infractions financières. Lors de cet avis, le Groupe de l'article 29 affirme sans ambages qu'«une obligation imposée par une loi ou un règlement étrangers qui exigeraient l'établissement de systèmes de signalement ne saurait être qualifiée d'obligation légals légitimant le traitement des données dans l'UE. Toute autre interprétation permettrait à des législations étrangères de contourner les règles fixées par l'UE avec la directive 95/46/CE».

28. En d'autres termes, les autorités de protection des données plaident clairement pour que l'exigence du caractère adéquat dans le cadre de flux transfrontières

---

[84] Avis du CEPD déjà cité.

[85] *JOCE*, 25 août 2000, L 215, pp. 7 et s.

[86] Avis n° 1/2006 du Groupe de l'article 29, concernant le Whistleblowing. Voir aussi sur ce système de signalement, l'avis de la CNIL, Document d'orientation pour la mise en œuvre de dispositifs d'alerte professionnelle, 10 nov. 2005 disponible sur le site de la CNIL.

de données, transferts rattachables au troisième pilier ne concerne pas seulement le transfert de données entre autorités publiques mais également entre entreprises et autorités publiques étrangères. En d'autres termes, même si le flux vers un pays tiers est jugé adéquat aux yeux du premier pilier il peut dans la mesure où la réglementation du pays tiers imposerait la communication de données à ses autorités publiques, être jugé alors inadéquat aux yeux du 3ème pilier. Sans doute, les entreprises n'apprécieront pas cette remise en cause dans la mesure où le non respect de la loi étrangère pour des raisons de protection des données risque de mettre à mal la continuation des opérations qui justifiaient le flux transfrontières et en tout cas l'expose à des sanctions sur le sol étranger.

On souligne par ailleurs tout l'intérêt qu'il y aurait de lier les décisions relatives au caractère adéquat sur base des deux piliers et la nécessité d'avoir une seule autorité se prononçant en la matière. Ce dernier point nous amène aux réflexions sur les risques de cette répartition des compétences suivant le pilier en cause.

2. Une division risquée

29. Nous avons précédemment insisté sur le fait de la nécessité d'une parfaite cohérence des réglementations des premier et troisième piliers. Or cette cohérence risque d'être mise à mal lorsqu' au niveau européen, on reconnaît l'existence de deux groupes consultatifs distincts. Ce danger a été aperçu par le CEPD qui plaide pour le renforcement des synergies entre les deux groupes (transmission systématique d'informations et présence du président du groupe de l'article 29).

Dans son rapport soumis au comité des libertés civiles, Martine Roure a également proposé un amendement en ce sens, arguant que la présence du président du groupe de l'article 29 aux réunions du nouveau groupe de travail renforcerait la communication et les échanges entre les deux groupes.

Sans doute serait-il préférable que les deux groupes soient identiques sous peine de renforcer une tendance au niveau national de consacrer pour le domaine de la police, de la Justice et de la sécurité publique une ou des autorités sectorielles développant une interprétation différente des principes de protection des données nonobstant leur identité.

3. Le risque d'atteinte au droit de recours effectif au niveau européen

30. La nouvelle proposition de Décision-Cadre s'inscrit dans le cadre du plan d'action adopté par le Conseil et la Commission mettant en oeuvre le programme de La Haye. Aux termes de ce plan d'action, la Commission devait présenter des *propo-*

sitions relatives (1) à l'établissement d'un principe de disponibilité[87] *des informations en matière répressive et (2) à des garanties adéquates et à des droits de recours effectifs pour le transfert des données à caractère personnel aux fins de la coopération policière et judiciaire en matière pénale.*

Une faiblesse majeure est cependant inhérente à l'adoption d'un instrument spécifique en matière de protection des données dans le troisième pilier. Il s'agit du risque de restreindre le droit des citoyens à un recours effectif.

A ce propos, il n'est sans doute pas inutile de rappeler que la compétence de la CJCE est limitée dans le cadre du troisième pilier. En atteste le fait que la procédure d'infraction n'est pas prévue pour les décisions relevant de la coopération policière et judiciaire[88]. Cela implique que ni la Commission, ni la CJCE ne peuvent jouer leurs responsabilités de garants dans le cadre du contrôle de la transposition du droit de l'Union des Etats Membres.

31. Cela a évidemment un impact sur l'effectivité du droit de recours des citoyens des Etats Membres dans la mesure où les institutions communautaires n'ont pas la compétence de sanctionner un Etat qui, par exemple, n'instituerait pas d'autorité de contrôle indépendante ou ne prévoirait pas de recours juridictionnel dans son droit national. D'autant plus que la CJCE n'est pas compétente pour vérifier la validité ou la proportionnalité d'opérations menées par la police ou d'autres services répressifs dans un État membre, ni pour statuer sur l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure.

Ensuite, à l'inverse de ce qui est prévu dans le cadre du pilier communautaire, la compétence de la CJCE de statuer à titre préjudiciel sur la validité et l'interprétation des décisions et conventions prises en matière de coopération policière et judiciaire en matière pénale est facultative[89]. Le Traité permet donc d'aboutir à un accès juridictionnel à géométrie très variable[90]. Ainsi, onze Etats Membres ne reconnaissent

---

[87] Le principe de disponibilité est un nouveau principe juridique important qui a été introduit dans le programme de La Haye et selon lequel les informations nécessaires dans le cadre de la lutte contre la criminalité doivent pouvoir traverser sans entraves les frontières intérieures de l'UE.

[88] Néanmoins, la Cour est compétente pour statuer sur tout différend entre les EM et la Commission concernant l'interprétation ou l'application (seulement) des conventions.

[89] De plus, selon le choix des Etats signataires, la saisine de la CJCE peut être ouverte à toutes les juridictions nationales ou réservée seulement aux juridictions nationales de dernier recours.

[90] Deux Etats Membres ont pris l'option que seule la juridiction de dernière instance peut interroger la Cour (HU, ESP); 3 Etats Membres (Finl., PT, Suède) ont pris l'option que toute juridiction peut poser une question, mais la dernière instance n'est pas tenue de porter l'affaire devant la Cour. 9 Etats Membres (AT, BE, CZ, DE, EL, FR, IT, Lux, NL) se sont alignés sur le modèle communautaire, c'est-à-dire que toute juridiction peut poser une question, et la juridiction de dernière instance est tenue de porter l'affaire devant la Cour.

tout simplement pas la compétence de la CJCE de connaître des recours préjudiciels dans les matières relevant du 3ème pilier[91].

Enfin, outre le mécanisme des questions préjudicielles, en cas d'atteinte à ses droits par les institutions communautaires, un citoyen lésé pourrait imaginer recourir à la procédure prévue par l'article 230 du Traité CE en arguant que ses droits ont été directement affectés par un accord tel que celui autorisant le transfert des données PNR. Cependant tant les conditions de ce recours, qui ont été interprétées de manière extrêmement restrictive par la CJCE[92], que le fait que ce recours doive impérativement être formé dans les 2 mois suivant la publication de l'acte, rendent cette voie peu plausible.

En matière de protection des données dans le 3ème pilier, la protection judiciaire limitée (et l'accès à géométrie variable à la CJCE) risquent de porter atteinte au droit des citoyens européens à un recours effectif garanti par l'article 47 de la Charte des Droits Fondamentaux et dont l'existence a été affirmé à maintes reprises par la CJCE[93]. Il lui restera, le cas échéant ayant épuisé l'ensemble des voies de recours internes, à invoquer devant la Cour strasbourgeoise, la violation de l'article 8 de la CEDH. Curieux retournement de situation là où l'adoption de la décision cadre avait pour but de renforcer l'effectivité de cette disposition du Conseil de l'Europe dont le traité de l'Union européenne garantit le respect des prescrits.

CONCLUSIONS

32. Dans l'attente d'une constitution européenne qui unifierait les piliers et permettrait d'aboutir à un seul texte affirmant les principes de la protection des données peu importe que le traitement se rattache au marché unique, à la coopération

---

[91] Il s'agit de CY, DK, EE, Irel., Lith, Latvia, MT, PL, Slovénie, Slovaquie, UK.

[92] En vertu de l'article 230 CE, les particuliers ont uniquement le droit d'attaquer les décisions individuelles des institutions européennes qui leur sont adressées. D'autres actions pourraient être contestées par des particuliers uniquement lorsque, exceptionnellement, ils sont en mesure de démontrer qu'ils sont «directement et individuellement concernés» par ces actions. En général, cela signifie que le demandeur doit prouver que l'action, même si elle ne lui est pas formellement adressée, constitue en fait une décision individuelle prise sous la forme d'un règlement ou d'une décision adressée à d'autres personnes et dont il est en fait le destinataire. Ce critère très strict rend presque impossible, en dehors de certains contextes spécifiques, que les particuliers contestent un acte pour lequel ils ne sont pas le destinataire officiel (par exemple, les actes généraux ou les actes destinés à d'autres personnes) même si ces actes affectent de manière très spécifique leur situation et leur causent des dommages graves ou irréparables. La CJCE elle-même dans son rapport de 1995 pour la Conférence Intergouvernementale de 1996, a indiqué que les dispositions de 230 CE pourraient ne pas être suffisantes pour assurer une protection judiciaire adéquate contre les violations des droits fondamentaux de l'homme par les institutions européennes.

[93] Voir notamment les arrêts de la CJCE Johnston v Chief Constable of the RUC, C-222/84 et Panayotova, C-327/02.

policière et pénale ou à la sûreté de l'Etat, nous saluons l'initiative européenne visant à la mise au point d'un texte général relatif à la protection des données dans le troisième pilier, et ce au-delà des règlements et textes divers visant des traitements bien particuliers. Ce texte repose tant sur une approche cohérente de la protection des données, reprenant avec bonheur les règles de transparence et de légitimation des traitements déjà définis dans le premier pilier mais en outre y ajoute certaines spécificités heureuses propres aux traitements du 3ème pilier, tel cette distinction entre données relatives à des infractions constatées et celles simplement suspectées. Comme le Commissaire européen à la protection des données le note, le texte initial en provenance de la Commission risque d'être un trompe l'œil s'il se limite aux seuls traitements de «coopération» entre autorités nationales et n'élargit pas son propos aux traitements opérés par ces autorités, s'il n'aborde pas de manière complète la réglementation de la coopération entre secteur privé et autorités publiques dans les tâches policières et de poursuite d'infractions.

33. Au-delà, nous avons relevé quelques difficultés liées à la distinction entre piliers qui affaiblissent la protection des données. Premièrement même si les lignes de démarcation entre les piliers semblent se dessiner progressivement, des zones d'ombre subsistent et le caractère indissociable de traitements conçus comme nécessaire à la poursuite d'une finalité unique soulève des difficultés lorsqu'artificiellement on rattache les uns au premier pilier, les autres au second ou troisième pilier. La question de l'effectivité des recours auprès des organes judiciaires européens en est sans doute un point à ne pas négliger. On songe également aux risques liés à la reconnaissance d'un double contrôleur au niveau européen et demain au niveau national, celui du premier pilier, celui du 3ème pilier. Leur jurisprudence et leur interprétation de principes pourtant communs risquent de créer des difficultés dans le futur, difficultés qui peuvent d'avoir des incidences très concrètes lorsqu'il s'agira d'analyser par exemple le caractère adéquat d'un système de protection offert par un pays étranger.

Qu'on ne s'y trompe pas, notre propos vis-à-vis de l'initiative européenne se veut celui d'un franc soutien à condition que l'effort soit élargi et que la distinction entre piliers sur la protection des données ne soit pas l'occasion d'un affaiblissement de cette protection. Sans doute peut-on rappeler ici l'enseignement de la jurisprudence de Strasbourg à propos de l'article 8 de la CEDH, référence omniprésente dans les documents européens: la Convention est un «instrument vivant à sens unique» [94], en d'autres termes, l'interprétation doit toujours aller dans le sens d'un renforcement des droits de l'Homme et non tendre à sa diminution.

---

[94] Sur ce caractère de la CEDH, lire les réflexions de R. A. Lawson, «The monitoring of Fundamental Rights in the Union as a Contribution to the European Legal space: the role of the European Court of Justice», in *Proceedings of the first REFGOV Open Conference,* O. de Schutter (ed.), May 2006, Brussels, to be published.